ON CYCLIC CODES OVER THE RING $\mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$

ABHAY KUMAR SINGH AND PRAMOD KUMAR KEWAT

Abstract. In this paper, we study cyclic codes over the ring $\mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$, where $u^k = 0$. We find a set of generator for these codes. We also study the rank, the dual and the Hamming distance of these codes.

1. Introduction

Let R be a ring. A linear code of length n over R is a R submodule of R^n. A linear code C of length n over R is cyclic if $(c_{n-1}, c_1, \ldots, c_0) \in C$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in C$. We can consider a cyclic code C of length n over R as an ideal in $R[x]/ < x^n - 1 >$ via the following correspondence

$$R^n \longrightarrow R[x]/ < x^n - 1 >,\ (c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}.$$

In recent time, cyclic codes over rings have been studied extensively because of their important role in algebraic coding theory. The structure of cyclic codes of odd length over rings has been discussed in a series of papers [6, 8, 10, 12]. In [7], [9] and [11], a complete structure of cyclic codes of odd length over $\mathbb{Z}_4$ has been presented. In [5], Blackford studied cyclic codes of length $n = 2k$, when k is odd. The cyclic codes of length a power of 2 over $\mathbb{Z}_4$ are studied in [1, 2]. Bonnecaze and Udaya in [6] studied cyclic codes of odd length over $R_2 = \mathbb{Z}_2 + u\mathbb{Z}_2, u^2 = 0$. In [3], Abualrub and Siap studied cyclic codes of an arbitrary length over $R_2 = \mathbb{Z}_2 + u\mathbb{Z}_2, u^2 = 0$ and over $R_3 = \mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2, u^3 = 0$. Al-Ashker and Hamoudeh in [4] extended some of the results in [3] to the ring $R_k = \mathbb{Z}_2 + u\mathbb{Z}_2 + \cdots + u^{k-1}\mathbb{Z}_2$, $u^k = 0$.

Let $R_k = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$ where p is a prime number and $u^k = 0$. In this paper, we discuss the structure of cyclic codes of arbitrary length over the ring R_k. We find a set of generators and a minimal spanning set for these codes. We also discuss about the rank and the Hamming distance of these codes. Recall that the Hamming weight of a codeword c is defined as the number of non-zero enteries of c and the Hamming distance of a code C is the smallest possible weight among all its non zero codewords.

Let C be a cyclic code over the ring $R_k = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$ where $u^k = 0$. The line of arguments we have used to find a set of genertors and a minimal spanning set of a code C are somewhat similar to those discussed in [3, 4]. Note that some slight modification needed in our case in order to find a set of genrator, e.g., the proofs of Lemmas 2.3 and 2.5 are slightly different from those discussed in [3, 4] where the proof is not very clear. Again, the line of arguments we have used to find minimum distance are similar to [3] but slightly different.

Key words and phrases. Cyclic codes.

The paper is organized as follows. In Section 2, we give a set of generators for the cyclic codes C over the ring $R_k = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p$ where $u^k = 0$. In Section 3, we find minimal spanning sets for these codes and dicuss about the rank. In Section 4, we find the minimum distance of these codes. In Section 5, we discuss some of the examples of these codes.

2. A generator for cyclic codes over the ring R_k

Let $R_k = \mathbb{Z}_p + u_k\mathbb{Z}_p + \cdots + u_k^{k-1}\mathbb{Z}_p,\ u_k^k = 0$. A cyclic code C of length n over R_k can be considered as an ideal in the $R_{k,n} = R_k[x]/ < x^n - 1 >$. Let C_k be a cyclic code of length n over R_k. We also consider C_k as an ideal in $R_{k,n}$. We define the map $\psi_{k-1} : R_k \longrightarrow R_{k-1}$ by $\psi_{k-1}(a_0 + u_ka_1 + \cdots + u_k^{k-1}a_{k-1}) = a_0 + u_{k-1}a_1 + \cdots + u_{k-1}^{k-2}a_{k-2}$, where $a_i \in \mathbb{Z}_p$. The map ψ_{k-1} is a ring homomorphism. We extend it to a homomorphism $\phi_{k-1} : C_k \longrightarrow R_{k-1,n}$ defined by

$$\phi_{k-1}(c_0+c_1x+\cdots+c_{n-1}x^{n-1}) = \psi_{k-1}(c_0)+\psi_{k-1}(c_1)x+\cdots+\psi_{k-1}(c_{n-1})x^{n-1}.$$

Let $J_{k-1} = \{r(x) \in \mathbb{Z}_p[x] : u_k^{k-1}r(x) \in \ker\phi_{k-1}\}$. It is easy to see that J_{k-1} is an ideal in $R_{1,n}$. Since $R_{1,n}$ is a principal ideal ring, we have $J_{k-1} =< a_{k-1}(x) >$ and $\ker\phi_{k-1} =< u_k^{k-1}a_{k-1}(x) >$ with $a_{k-1}(x)|(x^n - 1) \bmod p$.

Let C_{k-2} be a cyclic code of length n over R_{k-2}. We define the map $\psi_{k-2} : R_{k-1} \longrightarrow R_{k-2}$ by $\psi_{k-2}(a_0 + u_{k-1}a_1 + \cdots + u_{k-1}^{k-2}a_{k-2}) = a_0 + u_{k-2}a_1 + \cdots + u_{k-2}^{k-3}a_{k-3}$, where $a_i \in \mathbb{Z}_p$. The map ψ_{k-2} is a ring homomorphism. We extend it to a homomorphism $\phi_{k-2} : C_{k-1} \longrightarrow R_{k-2,n}$ defined by

$$\phi_{k-2}(c_0+c_1x+\cdots+c_{n-1}x^{n-1}) = \psi_{k-2}(c_0)+\psi_{k-2}(c_1)x+\cdots+\psi_{k-2}(c_{n-1})x^{n-1}.$$

Let $J_{k-2} = \{r(x) \in \mathbb{Z}_p[x] : u_{k-1}^{k-2}r(x) \in \ker\phi_{k-2}\}$. We see that J_{k-2} is an ideal in $R_{1,n}$. As above, we have $J_{k-2} =< a_{k-2}(x) >$ and $\ker\phi_{k-2} =< u_{k-1}^{k-2}a_{k-2}(x) >$ with $a_{k-2}(x)|(x^n - 1) \bmod p$.

We continue in the same way as above and define $\psi_{k-3}, \psi_{k-4}, \cdots, \psi_2$ and $\phi_{k-3}, \phi_{k-4}, \cdots, \phi_2$. We define $\psi_1 : R_2 \longrightarrow R_1 = \mathbb{Z}_p$ by $\psi_k(a_0 + u_2a_1) = a_0$. The map ψ_1 is a ring homomorphism. We extend ψ_1 to a homomorphism $\phi_1 : C_2 \longrightarrow R_{1,n}$ defined by

$$\phi_1(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) = \psi_1(c_0) + \psi_1(c_1)x + \cdots + \psi_1(c_{n-1})x^{n-1}.$$

As above, we have $\ker\phi_1 =< u_2a_1(x) >$ with $a_1(x)|(x^n - 1) \bmod p$. The image of ϕ_1 is an ideal in $R_{1,n}$ and hence a cyclic code in $\mathbb{Z}_p$. Since $R_{1,n}$ is a principal ideal ring, the image of ϕ_1 is generated by some $g(x) \in \mathbb{Z}_p[x]$ with $g(x)|(x^n - 1)$. Hence, we have $C_2 =< g(x) + u_2p(x), u_2a_1(x) >$ for some $p(x) \in \mathbb{Z}_p[x]$. We have

$$\phi_1(\frac{x^n - 1}{g(x)}(g(x) + u_2p(x)) = \phi_1(u_2p(x)\frac{x^n - 1}{g(x)}) = 0.$$

Therefore, $u_2p(x)\frac{x^n - 1}{g(x)} \in \ker\phi_1 =< u_2a_1(x) >$. Hence, $a_1(x)|p(x)\frac{x^n - 1}{g(x)}$. Also we have $u_2g(x) \in \ker\phi_1$. This implies that $a_1(x)|g(x)$.

Lemma 2.1. *Let C_2 be a cyclic code over $R_2 = \mathbb{Z}_p + u\mathbb{Z}_p, u^2 = 0$. If $C_2 =< g(x) + up(x), ua_1(x) >$, and $g(x) = a_1(x)$ with $\deg\ g(x) = r$, then*

$$C_2 =< g(x) + up(x) > \ \text{and}\ (g(x) + up(x))|(x^n - 1)\ \text{in}\ R_2.$$

Proof. We have $u(g(x) + up(x)) = ug(x)$ and $g(x) = a(x)$. It is clear that $C_2 \subset< g(x) + up(x) >$. Hence, $C_2 =< g(x) + up(x) >$. By the division algorithm, we have

$$x^n - 1 = (g(x) + up(x))q(x) + r(x), \text{ where } r(x) = 0 \text{ or } \deg\ r(x) < r.$$

Since $r(x) \in C_2$, we have $r(x) = 0$ and hence $(g(x)+up(x))|(x^n-1)$ in R_2. □

Note that the image of ϕ_2 is an ideal in $R_{2,n}$, hence a cyclic code over R_2. Therefore, we have $\text{Im}(\phi_2) =< g(x)+u_2p_1(x), u_2a_1(x) >$ with $a_1(x)|g(x)|(x^n-1)$ and $a_1(x)|p_1(x)(\dfrac{x^n-1}{g(x)})$. Also, we have $\ker\phi_2 =< u_3^2a_2(x) >$ with $a_2(x)|(x^n-1) \bmod p$ and $u_3^2a_1(x) \in \ker\phi_2$. As above, the cyclic code C_3 over R_3 is given by

$$C_3 =< g + u_3p_1(x) + u_3^2p_2(x), u_3a_1(x) + u_3^2q_1(x), u_3^2a_2(x) >$$

with $a_2(x)|a_1(x)|g(x)|(x^n-1)$, $a_1(x)|p_1(x)(\dfrac{x^n-1}{g(x)}) \bmod p$, $a_2(x)|q_1(x)(\dfrac{x^n-1}{a_1(x)})$, $a_2(x)|p_1(x)\dfrac{x^n-1}{g(x)}$ and $a_2(x)|p_2(x)(\dfrac{x^n-1}{g(x)})(\dfrac{x^n-1}{a_1(x)})$. We may assume that $\deg\ p_2(x) < \deg a_2(x)$, $\deg q_1(x) < \deg a_2(x)$ and $\deg\ p_1(x) < \deg a_1(x)$ because g.c.d.$(a, b) =$ g.c.d.$(a, b + da)$ for any d. We have the following lemma.

Lemma 2.2. *Let C_3 be a cyclic code over $R_3 = \mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p, u^3 = 0$. If $C_3 =< g + up_1(x) + u^2p_2(x), ua_1(x) + u^2q_1(x), u^2a_2(x) >$, and $a_2(x) = g(x)$, then $C_3 =< g + up_1(x) + u^2p_2(x) >$ and $(g + up_1(x) + u^2p_2(x))|(x^n - 1)$ in R_3.*

Proof. Since $a_2(x) = g(x)$, we have $a_1(x) = a_2(x) = g(x)$. From Lemma 2.1, we get $(g(x)+up(x)|(x^n-1)$ in R_2, and $C_3 =< g+up_1(x)+u^2p_2(x), u^2a_2(x) >$. The rest of the proof is similar to Lemma 2.1. □

Lemma 2.3. *Let C_3 be a cyclic code over $R_3 = \mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p, u^3 = 0$. If n is relatively prime to p, then $C_3 =< g(x), ua_1(x), u^2a_2(x) > = < g(x) + ua_1(x) + u^2a_2(x) >$ over R_3.*

Proof. Since n is relatively prime to p, the polynomial $x^n - 1$ factors uniquely into a product of distinct irreducible polynomials. This gives,

$$\text{g.c.d.}(a_1(x), \frac{(x^n-1)}{g(x)}) = \text{g.c.d.}(a_2(x), \frac{(x^n-1)}{a_1(x)}) = \text{g.c.d.}(a_2(x), \frac{(x^n-1)}{g(x)}) = 1.$$

Since $a_1(x)|p_1(x)(\dfrac{x^n-1}{g(x)})$, we get $a_1(x)|p_1(x)$. But $\deg p_1(x) < \deg a_1(x)$, hence $p_1(x) = 0$. We have $a_2(x)|q_1(x)(\dfrac{x^n-1}{a_1(x)})$ and $a_2(x)|p_2(x)(\dfrac{x^n-1}{g(x)})(\dfrac{x^n-1}{a_1(x)})$, this gives $a_2(x)|q_1(x)$ and $a_2(x)|p_2(x)$. But $\deg q_1(x) < \deg a_2(x)$ and $\deg p_2(x) <$

deg$a_2(x)$, hence $p_2(x) = q_1(x) = 0$. So, $C_3 =< g(x), ua_1(x), u^2a_2(x) >$. Let $h(x) = g(x) + ua_1(x) + u^2a_2(x)$. Then

$$u^2h(x) = u^2g(x),\ \frac{x^n-1}{a_1(x)}h(x) = \frac{x^n-1}{a_1(x)}u^2a_2(x),\ \text{and}$$

$$u\frac{x^n-1}{g(x)}h(x) = \frac{x^n-1}{g(x)}u^2a_1(x) \in < h(x) > .$$

Since n is relatively prime to p, we have

$$\text{g.c.d.}\left(g(x), \frac{(x^n-1)}{g(x)}\right) = \text{g.c.d.}\left(a_1(x), \frac{(x^n-1)}{a_(x)}\right) = 1.$$

Hence, $1 = f_1(x)\dfrac{(x^n-1)}{g(x)} + f_2(x)g(x)$, for some polynomial $f_1(x)$ and $f_2(x)$, and $1 = m_1(x)\dfrac{(x^n-1)}{a_1(x)} + m_2(x)a_1(x)$, for some polynomial $m_1(x)$ and $m_2(x)$. Therefore, $u^2a_1(x) = u^2a_1(x)f_1(x)\dfrac{(x^n-1)}{g(x)} + u^2a_1(x)f_2(x)g(x) \in < h(x) >$, $u^2a_2(x) = u^2a_2(x)m_1(x)\dfrac{(x^n-1)}{a_1(x)} + u^2a_2(x)m_2(x)a_1(x) \in < h(x) >$ and hence $g(x) + ua_1(x) \in < h(x) >$. We have $(g(x) + ua_1(x))^2 = g(x)^2 + 2ug(x)a_1(x) + u^2a_1(x)^2$. Since $u^2a_1(x)^2 \in < h(x) >$, we have $g(x)^2 + 2ua_1(x)g(x) \in < h(x) >$ and $ug(x)^2 + 2u^2a_1(x)g(x) \in < h(x) >$. So, $ug(x)^2 \in < h(x) >$. We have $ug(x) = uf_2(x)g(x)^2$. Hence, $ug(x) \in < h(x) >$. We have

$$\frac{x^n-1}{g(x)}h(x) = \frac{x^n-1}{g(x)}ua_1(x) + \frac{x^n-1}{g(x)}u^2a_2(x).$$

Since $u^2a_2(x) \in < h(x) >$, this gives $\dfrac{x^n-1}{g(x)}ua_1(x) \in < h(x) >$. We also have

$$ua_1(x) = f_1(x)\frac{(x^n-1)}{g(x)}ua_1(x) + f_2(x)ug(x)a_1(x).$$

This gives, $ua_1(x) \in < h(x) >$ and hence $g(x) \in < h(x) >$. Therefore, $C_3 = < g(x), ua_1(x), u^2a_2(x) > = < g(x) + ua_1(x) + u^2a_2(x) >$. $\square$

Note that the image of ϕ_3 is an ideal in $R_{3,n}$, hence a cyclic code over R_3. Therefore, we have $\text{Im}(\phi_3) =< g+u_3p_1(x)+u_3^2p_2(x), u_3a_1(x)+u_3^2q_1(x), u_3^2a_2(x) >$ with $a_2(x)|a_1(x)|g(x)|(x^n-1)$ and $a_1(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$, $a_2(x)|q_1(x)\left(\frac{x^n-1}{a_2(x)}\right)$ and $a_1(x)|p_2(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{a_1(x)}\right)$. Also, we have ker$\phi_3 =< u_4^3a_3(x) >$ with $a_3(x)|(x^n-1)$ mod p and $u_4^3a_2(x) \in$ kerϕ_3. As above, the cyclic code C_4 over R_4 is given by $C_4 =< g+u_4p_1(x)+u_4^2p_2(x)+u_4^3p_3(x), u_4a_1(x)+u_4^2q_1(x)+u_4^3q_2(x), u_4^2a_2(x)+u_4^3l_1(x), u_4^3a_3(x) >$ with $a_3(x)|a_2(x)|a_1(x)|g(x)|(x^n-1)$, $a_1(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$ mod p, $a_2(x)|q_1(x)\left(\frac{x^n-1}{a_1(x)}\right)$, $a_2(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$, $a_2(x)|p_2(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{a_1(x)}\right)$, $a_3(x)|l_1(x)\left(\frac{x^n-1}{a_2(x)}\right)$, $a_3(x)|q_2(x)\left(\frac{x^n-1}{q_1(x)}\right)\left(\frac{x^n-1}{a_1(x)}\right)$ and $a_3(x)|p_3(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{a_2(x)}\right)\times$

$\left(\frac{x^n-1}{a_1(x)}\right)$. We may assume that $\deg p_3(x) < \deg a_3(x)$, $\deg q_2(x) < \deg a_3(x)$, $\deg l_1(x) < \deg a_3(x)$, $\deg\ p_2(x) < \deg a_2(x)$, $\deg q_1(x) < \deg a_2(x)$ and $\deg\ p_1(x) < \deg a_1(x)$ because g.c.d.$(a, b) =$ g.c.d.$(a, b + da)$ for any d. We have the following lemma.

Lemma 2.4. *Let C_4 be a cyclic code over $R_4 = \mathbb{Z}_p+u\mathbb{Z}_p+u^2\mathbb{Z}_p+u^3\mathbb{Z}_p, u^4 = 0$. If $C_4 =< g + up_1(x) + u^2p_2(x) + u^3p_3(x), ua_1(x) + u^2q_1(x) + u^3q_2(x), u^2a_2(x) + u^3l_1(x), u^3a_3(x) >$, and $a_3(x) = g(x)$, then $C_4 =< g + up_1(x) + u^2p_2(x) + u^3p_3(x) >$ and $(g + up_1(x) + u^2p_2(x) + u^3p_3(x))|(x^n - 1)$ in R_4.*

Proof. Since $a_3(x) = g(x)$, we have $a_1(x) = a_2(x) = a_3(x) = g(x)$. From Lemma 2.2, we get $(g(x) + up_1(x) + u^2p_2(x))|(x^n - 1)$ in R_3, and $C_4 =< g+up_1(x)+u^2p_2(x)+u^3p_3(x), ua_1(x)+u^2q_1(x)+u^3q_2(x), u^3a_3(x) >$. The rest of the proof is similar to Lemma 2.2. □

Lemma 2.5. *Let C_4 be a cyclic code over $R_4 = \mathbb{Z}_p+u\mathbb{Z}_p+u^2\mathbb{Z}_p+u^3\mathbb{Z}_p, u^4 = 0$. If n is relatively prime to p, then $C_4 =< g(x), ua_1(x), u^2a_2(x), u^3a_3(x) > = < g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x) >$ over R_4.*

Proof. The proof is similar to Lemma 2.3. Since n is relatively prime to p, the polynomial $x^n - 1$ factors uniquely into a product of distinct irreducible polynomials. This gives,

$$\text{g.c.d.}\left(a_1(x), \tfrac{(x^n-1)}{g(x)}\right) = \text{g.c.d.}\left(a_2(x), \tfrac{(x^n-1)}{a_1(x)}\right) = \text{g.c.d.}\left(a_2(x), \tfrac{(x^n-1)}{g(x)}\right) = 1,$$

$$\text{g.c.d.}\left(a_3(x), \tfrac{(x^n-1)}{a_2(x)}\right) = \text{g.c.d.}\left(a_3(x), \tfrac{(x^n-1)}{a_1(x)}\right) = \text{g.c.d.}\left(a_3(x), \tfrac{(x^n-1)}{g(x)}\right) = 1.$$

Since $a_1(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$, we get $a_1(x)|p_1(x)$. But $\deg p_1(x) < \deg a_1(x)$, hence $p_1(x) = 0$. We have $a_2(x)|q_1(x)\left(\frac{x^n-1}{a_1(x)}\right)$ and $a_2(x)|p_2(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{a_1(x)}\right)$, this gives $a_2(x)|q_1(x)$ and $a_2(x)|p_2(x)$. But $\deg q_1(x) < \deg a_2(x)$ and $\deg p_2(x) < \deg a_2(x)$, hence $p_2(x) = q_1(x) = 0$. Similarly, $p_3(x) = q_2(x) = l_1(x) = 0$. So, $C_4 =< g(x), ua_1(x), u^2a_2(x), u^3a_3(x) >$. Let $h(x) = g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x)$. Then

$$u^3h(x) = u^3g(x),\ \frac{x^n-1}{a_2(x)}h(x) = \frac{x^n-1}{a_2(x)}u^3a_3(x),$$

$$u\frac{x^n-1}{a_1(x)}h(x) = \frac{x^n-1}{a_1(x)}u^3a_2(x) \text{ and } u^2\frac{x^n-1}{g(x)}h(x) = \frac{x^n-1}{g(x)}u^3a_1(x) \in< h(x) > .$$

Since n is relatively prime to p, we have

$$\text{g.c.d.}\left(g(x), \tfrac{(x^n-1)}{g(x)}\right) = \text{g.c.d.}\left(a_1(x), \tfrac{(x^n-1)}{a_1(x)}\right) = \text{g.c.d.}\left(a_2(x), \tfrac{(x^n-1)}{a_2(x)}\right) = 1.$$

Hence, $1 = f_1(x)\frac{(x^n-1)}{g(x)} + f_2(x)g(x)$, for some polynomials $f_1(x)$ and $f_2(x)$, $1 = m_1(x)\frac{(x^n-1)}{a_1(x)} + m_2(x)a_1(x)$, for some polynomials $m_1(x)$ and $m_2(x)$ and $1 = n_1(x)\frac{(x^n-1)}{a_2(x)} + n_2(x)a_2(x)$, for some polynomials $n_1(x)$ and $n_2(x)$. Therefore,

$$u^3a_1(x) = u^3a_1(x)f_1(x)\tfrac{(x^n-1)}{g(x)} + u^3a_1(x)f_2(x)g(x) \in < h(x) >,$$
$$u^3a_2(x) = u^3a_2(x)m_1(x)\tfrac{(x^n-1)}{a_1(x)} + u^3a_2(x)m_2(x)a_1(x) \in < h(x) > \text{ and}$$
$$u^3a_3(x) = u^3a_3(x)n_1(x)\tfrac{(x^n-1)}{a_2(x)} + u^3a_3(x)n_2(x)a_2(x) \in < h(x) > .$$

Hence, $g(x) + ua_1(x) + u^2a_2(x) \in < h(x) >$. We have $(g(x) + ua_1(x) + u^2a_2(x))^2 = g(x)^2 + u^2a_1(x)^2 + 2ug(x)a_1(x) + 2u^2g(x)a_2(x) + 2u^3a_1(x)a_2(x)$. Since $u^3a_2(x) \in < h(x) >$, we have $g(x)^2+u^2a_1(x)^2+2ua_1(x)g(x)+2u^2g(x)a_2(x) \in < h(x) >$ and hence $u^2g(x)^2 \in < h(x) >$. We have $u^2g(x) = u^2f_2(x)g(x)^2$. Hence, $u^2g(x) \in < h(x) >$. We have

$$\frac{x^n-1}{a_1(x)}h(x) = \frac{x^n-1}{a_1(x)}u^2a_2(x) + \frac{x^n-1}{a_1(x)}u^3a_3(x) \text{ and}$$

$$u\frac{x^n-1}{g(x)}h(x) = \frac{x^n-1}{g(x)}u^2a_1(x) + \frac{x^n-1}{g(x)}u^3a_2(x).$$

This gives, $\dfrac{x^n-1}{g(x)}u^2a_1(x) \in < h(x) >$ and $\dfrac{x^n-1}{a_1(x)}u^2a_2(x) \in < h(x) >$. We have

$$u^2a_1(x) = f_1(x)\frac{(x^n-1)}{g(x)}u^2a_1(x) + f_2(x)u^2g(x)a_1(x).$$

Therefore, $u^2a_1(x) \in < h(x) >$. We also have

$$u^2a_2(x) = m_1(x)\frac{(x^n-1)}{a_1(x)}u^2a_2(x) + u^2m_2(x)a_1(x)a_2(x).$$

Therefore, $u^2a_2(x) \in < h(x) >$. Hence, $g(x) + ua_1(x) \in < h(x) >$. The rest of the proof is similar to Lemma 2.3, but for readers convenience we repeat the proof here. We have $(g(x) + ua_1(x))^2 = g(x)^2 + 2ug(x)a_1(x) + u^2a_1(x)^2$. Since $u^2a_1(x) \in < h(x) >$, we have $g(x)^2 + 2ua_1(x)g(x) \in < h(x) >$ and $ug(x)^2 + 2u^2a_1(x)g(x) \in < h(x) >$. So, $ug(x)^2 \in < h(x) >$. We have $ug(x) = uf_2(x)g(x)^2$. Hence, $ug(x) \in < h(x) >$. We have

$$\frac{x^n-1}{g(x)}h(x) = \frac{x^n-1}{g(x)}ua_1(x) + \frac{x^n-1}{g(x)}u^2a_2(x) + \frac{x^n-1}{g(x)}u^3a_3(x).$$

Since $u^2a_2(x), u^3a_3(x) \in < h(x) >$, this gives $\dfrac{x^n-1}{g(x)}ua_1(x) \in < h(x) >$. We also have

$$ua_1(x) = f_1(x)\frac{(x^n-1)}{g(x)}ua_1(x) + f_2(x)ug(x)a_1(x).$$

This gives, $ua_1(x) \in < h(x) >$ and hence $g(x) \in < h(x) >$. Therefore, $C_4 = < g(x), ua_1(x), u^2a_2(x), u^3a_3(x) > = < g(x) + ua_1(x) + u^2a_2(x) + u^3a_3(x) >$. This proves the lemma. □

Following the same process as above and by induction on k, we get the following theorem.

Theorem 2.6. *Let C_k be a cyclic code over $R_k = \mathbb{Z}_p + u\mathbb{Z}_p + u^2\mathbb{Z}_p + \cdots + +u^{k-1}\mathbb{Z}_p, u^k = 0$.*

(1) *If n is relatively prime to p, then we have* $C_k =< g(x), ua_1(x), u^2a_2(x), \ldots, u^{k-1}a_{k-1}(x) > \; = \; < g(x) + ua_1(x) + u^2a_2(x) + \cdots + u^{k-1}a_{k-1}(x) >$ *over* R_k.

(2) *If n is not relatively prime to p, then*

(a) $C_k =< g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x) >$ *where* $g(x)$ *and* $p_i(x)$ *are polynomials in* $\mathbb{Z}_p[x]$ *for each* $i = 1, 2, \ldots, k-1$ *with* $g(x)|(x^n-1) \mod p$, $(g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x))|(x^n-1)$ *in* R_k *and* $\deg p_i < \deg p_{i-1}$ *for all* $1 \leq i \leq k$. Or

(b) $C_k =< g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x), u^{k-1}a_{k-1}(x) >$ *where* $a_{k-1}(x)|g(x)|(x^n-1) \mod p$, $g(x)+up(x)|(x^n-1)$ *in* R_2, $g(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$ *and* $a_{k-1}(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$, $a_{k-1}(x)|p_2(x)\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{g(x)}\right), \ldots,$ $a_{k-1}(x)|p_{k-1}(x)\underbrace{\left(\frac{x^n-1}{g(x)}\right)\cdots\left(\frac{x^n-1}{g(x)}\right)}_{k-1 \text{ times}}$ *and* $\deg p_{k-1}(x) < \deg a_{k-1}(x)$. Or

(c) $C_k =< g+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x), ua_1(x)+u^2q_1(x)+\cdots+u^{k-1}q_{k-2}(x), u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x), \ldots, u^{k-2}a_{k-2}(x) + u^{k-1}t_1(x), u^{k-1}a_{k-1}(x) >$ *with* $a_{k-1}(x)|a_{k-2}(x)|\cdots|a_2(x)|a_1(x)|g(x)|(x^n-1) \mod p$ $a_{k-2}(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right), \ldots, a_{k-1}|t_1(x)\left(\frac{x^n-1}{a_{k-2}(x)}\right), \ldots, a_{k-1}|p_{k-1}\times\left(\frac{x^n-1}{g(x)}\right)\cdots\left(\frac{x^n-1}{a_{k-2}(x)}\right)$. *Moreover,* $\deg p_{k-1}(x) < \deg a_{k-1}(x), \ldots, \deg t_1(x) < a_{k-1}(x), \ldots,$ *and* $\deg p_1(x) < \deg a_{k-2}(x)$.

3. Ranks and minimal spanning sets

Theorem 3.1. *Let n is not relatively prime to p. Let C_2 be a cyclic code of length n over* $R_2 = \mathbb{Z}_p + u\mathbb{Z}_p, u^2 = 0$.

(1) *If* $C_2 =< g(x)+up(x) >$ *with deg* $g(x) = r$ *and* $(g(x)+up(x))|(x^n-1)$, *then* C_2 *is a free module with rank* $n-r$ *and a basis* $B_1 = \{g(x)+up(x), x(g(x)+up(x)), \ldots, x^{n-r-1}(g(x)+up(x))\}$, *and* $|C_2| = p^{2n-2r}$.

(2) *If* $C_2 =< g(x) + up(x), ua(x) >$ *with deg* $g(x) = r$ *and deg* $a(x) = t$, *then* C_2 *has rank* $n-t$ *and a minimal spanning set* $B_2 = \{g(x)+up(x), x(g(x)+up(x)), \ldots, x^{n-r-1}(g(x)+up(x)), ua(x), xua(x), \ldots, x^{r-t-1}ua(x)\}$, *and* $|C_2| = p^{2n-r-t}$.

Proof. (1) Suppose $x^n - 1 = (g(x) + up(x))(h(x) + uh_1(x))$ over R_2. Let $c(x) \in C_2 =< g(x) + up(x) >$, then $c(x) = (g(x) + up(x))f(x)$ for some polynomial $f(x)$. If deg $f(x) \leq n-r-1$, then $c(x)$ can be written as linear combinations of elements of B_1. Otherwise by the division algorithm there exist polynomials $q(x)$ and $r(x)$ such that

$$f(x) = \left(\frac{x^n-1}{g(x)+up(x)}\right)q(x) + r(x) \text{ where } r(x) = 0 \text{ or } \deg r(x) \leq n-r-1.$$

This gives,

$$\begin{aligned}(g(x)+up(x))f(x) =&(g(x)+up(x))\left(\left(\frac{x^n-1}{g(x)+up(x)}\right)q(x)+r(x)\right)\\ =&(g(x)+up(x))r(x).\end{aligned}$$

Since deg $r(x) \leq n-r-1$, this shows that B_1 spans C_2. Now we only need to show that B_1 is linearly independent. Let $g(x) = g_0 + g_1x + \cdots + g_rx^r$ and $p(x) = p_0 + p_1x + \cdots + p_lx^l$, $g_0 \in \mathbb{Z}_p^\times, g_i, p_{i-1} \in \mathbb{Z}_p, i \geq 1$. Suppose

$$(g(x)+up(x))c_0 + x(g(x)+up(x))c_1 + \cdots + x^{n-r-1}(g(x)+up(x))c_{n-r-1} = 0.$$

By comparing the coefficients in the above equation, we get

$$(g_0 + up_0)c_0 = 0. \text{ (constant coefficient)}$$

Since $(g_0 + up_0)$ is unit, we get $c_0 = 0$. Thus,

$$x(g(x)+up(x))c_1 + \cdots + x^{n-r-1}(g(x)+up(x))c_{n-r-1} = 0.$$

Again comparing the coefficients, we get

$$(g_0 + up_0)c_1 = 0. \text{ (coefficient of } x).$$

As above, this gives $c_1 = 0$. Continuing in this way we get that $c_i = 0$ for all $i = 0, 1. \ldots, n-r-1$. Therefore, the set B_1 is linearly independent and hence a basis for C_2.

(2) If $C_2 =< g(x)+up(x), ua(x) >$ with deg $g(x) = r$ and deg $a(x) = t$. The lowest degree polynomial in C_2 is $ua(x)$. It is suffices to show that B_2 spans $B = \{g(x)+up(x), x(g(x)+up(x)), \ldots, x^{n-r-1}(g(x)+up(x)), ua(x), xua(x), \ldots, x^{n-t-1}ua(x)\}$. We first show that $ux^{r-t}a(x) \in \text{span}(B_2)$. Let the leading coefficients of $x^{r-t}a(x)$ be a_0 and of $g(x)+up(x)$ be g_0. There exists a constant $c_0 \in \mathbb{Z}_p$ such that $a_0 = c_0g_0$. Then we have

$$ux^{r-t}a(x) = uc_0(g(x)+up(x)) + um(x),$$

where $um(x)$ is a polynomial in C_2 of degree less than r. Since $C_2 =< g(x)+up(x), ua(x) >$, any polynomial in C_2 must have degree greater or equal to deg $a(x) = t$. Hence, $t \leq$ deg $m(x) < r$ and

$$um(x) = \alpha_0ua(x) + \alpha_1xua(x) + \cdots + \alpha_{r-t-1}x^{r-t-1}ua(x).$$

Thus, $ux^{r-t}a(x) \in \text{span}(B_2)$. Inductively, we can show that $ux^{r-t+1}a(x), \ldots, ux^{n-t-1}a(x) \in \text{span}(B_2)$. Hence B_2 is a generating set. As in (1), by comparing the coefficients we can see that B_2 is linearly independent. Therefore, B_2 is a minimal spanning set and $|C_2| = p^{2n-r-t}$. $\square$

Following the same process as in the above theorem, we can find the rank and the minimal spanning set of any cyclic code over the ring $R_k, k \geq 1$.

Theorem 3.2. *Let n is not relatively prime to p. Let C_k be a cyclic code of length n over $R_k = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p, u^k = 0$. We assume the constraints on the generator polynomials of C_k as in Theorem* 2.6.

(1) *If* $C_k =< g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x) >$ *with deg* $g(x) = r$, *then* C_k *is a free module with rank* $n-r$ *and a basis* $B_1 = \{g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x), x(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x)), \ldots, x^{n-r-1}(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x))\}$.

(2) *If* $C_k =< g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x), ua_1(x)+u^2q_1(x)+\cdots+u^{k-1}q_{k-2}(x), u^2a_2(x)+u^3l_1(x)+\cdots+u^{k-1}l_{k-3}(x), \ldots, u^{k-2}a_{k-2}(x)+u^{k-1}t_1(x), u^{k-1}a_{k-1}(x) >$ *with deg* $g(x) = r_1$, *deg* $a_1(x) = r_2$, *deg* $a_2(x) = r_3, \ldots,$ *deg* $a_{k-1}(x) = r_k$, *then* C_k *has rank* $n-r_k$ *and a minimal spanning set* $B_2 = \{g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x), x(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x)), \ldots, x^{n-r_1-1}(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x)), ua_1(x)+u^2q_1(x)+\cdots+u^{k-1}q_{k-2}(x), x(ua_1(x)+u^2q_1(x)+\cdots+u^{k-1}q_{k-2}(x)), \ldots, x^{r_1-r_2-1}(ua_1(x)+u^2q_1(x)+\cdots+u^{k-1}q_{k-2}(x)), u^2a_2(x)+u^3l_1(x)+\cdots+u^{k-1}l_{k-3}(x), x(u^2a_2(x)+u^3l_1(x)+\cdots+u^{k-1}l_{k-3}(x)), \ldots, x^{r_2-r_3-1}(u^2a_2(x)+u^3l_1(x)+\cdots+u^{k-1}l_{k-3}(x)), \ldots, u^{k-1}a_{k-1}(x), xu^{k-1}a_{k-1}(x), \ldots, x^{r_{k-1}-r_k-1}u^{k-1}a_{k-1}(x)\}$.

(3) *If* $C_k =< g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x), u^{k-1}a_{k-1}(x) >$ *with deg* $g(x) = r$ *and deg* $a_{k-1}(x) = t$, *then* C_k *has rank* $n-t$ *and a minimal spanning set* $B_3 = \{g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x), x(g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x)), \ldots, x^{n-r-1}(g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x)), u^{k-1}a_{k-1}(x), xu^{k-1}a_{k-1}(x), \ldots, x^{r-t-1}u^{k-1}a_{k-1}(x)\}$.

Proof. (1) The proof is same as in Theorem 3.1. Suppose $x^n-1=$

$$(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x))(h(x)+uh_1(x)+\cdots+u^{k-1}h_{k-1}(x))$$

over R_k. Suppose $x^n-1 = (g(x)+up(x))(h(x)+uh_1(x))$ over R_2. Let $c(x) \in C_k =< g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x) >$, then $c(x) = (g(x)+up_1(x)+u^2p_2(x)+\cdots+u^{k-1}p_{k-1}(x))f(x)$ for some polynomial $f(x)$. If deg $f(x) \le n-r-1$, then $c(x)$ can be written as linear combinations of elements of B_1. Otherwise by the division algorithm there exist polynomials $q(x)$ and $r(x)$ such that

$$f(x) = \left(\frac{x^n-1}{g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x)}\right)q(x)+r(x)$$

where $r(x) = 0$ or deg $r(x) \le n-r-1$. This gives,

$$(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x))f(x) = (g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x))r(x).$$

Since deg $r(x) \le n-r-1$, this shows that B_1 spans C_k. Now we only need to show that B_1 is linearly independent. Let $g(x) = g_0+g_1x+\cdots+g_rx^r$ and $p_1(x) = p_{1,0}+p_{1,1}x+\cdots+p_{1,l_1}x^{l_1}$, $p_2(x) = p_{2,0}+p_{2,1}x+\cdots+p_{1,l_2}x^{l_2}, \ldots,$ $p_{k-1}(x) = p_{k-1,0}+p_{k-1,1}x+\cdots+p_{k-1,l_{k-1}}x^{l_{k-1}}$, $g_0 \in \mathbb{Z}_p^\times, g_i, p_{j,i-1} \in \mathbb{Z}_p, i,j \ge 1$. Suppose $(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x))c_0 + x(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x))c_1+\cdots+x^{n-r-1}(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x))c_{n-r-1} = 0$. By comparing the coefficients in the above equation, we get

$$(g_0+up_{1,0}+\cdots+u^{k-1}p_{k-1,0})c_0 = 0. \text{ (constant coefficient)}$$

Since $(g_0+up_{1,0}+\cdots+u^{k-1}p_{k-1,0})$ is unit, we get $c_0 = 0$. Thus, $x(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x))c_1+\cdots+x^{n-r-1}(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x))c_{n-r-1} = 0$. Again comparing the coefficients, we get

$$(g_0 + up_{1,0} + \cdots + u^{k-1}p_{k-1,0})c_1 = 0. \text{ (coefficient of } x).$$

As above, this gives $c_1 = 0$. Continuing in this way we get that $c_i = 0$ for all $i = 0, 1. \ldots, n-r-1$. Therefore, the set B_1 is linearly independent and hence a basis for C_k.
(2) If $C_k =< g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x), ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x), u^2a_2(x)+u^3l_1(x)+\cdots+u^{k-1}l_{k-3}(x), \ldots, u^{k-2}a_{k-2}(x)+u^{k-1}t_1(x), u^{k-1}a_{k-1}(x) >$ with deg $(g(x)+up_1(x)+\cdots+u^{k-1}p_{k-1}(x)) = r_1$, deg $(ua_1(x)+u^2q_1(x)+\cdots+u^{k-1}q_{k-2}(x)) = r_2$, deg $(u^2a_2(x)+u^3l_1(x)+\cdots+u^{k-1}l_{k-3}(x)) = r_3, \ldots,$ and deg $(u^{k-1}a_{k-1}(x)) = r_k$. The lowest degree polynomial in C_k is $u^{k-1}a_{k-1}(x)$. It is suffices to show that B_2 spans $B = \{g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x), x(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)), \ldots, x^{n-r_1-1}(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)), ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x), x(ua_1(x) + u^2q_1(x) + \cdots+u^{k-1}q_{k-2}(x)), \ldots, x^{r_1-r_2-1}(ua_1(x)+u^2q_1(x)+\cdots+u^{k-1}q_{k-2}(x)), u^2a_2(x)+u^3l_1(x)+\cdots+u^{k-1}l_{k-3}(x), x(u^2a_2(x)+u^3l_1(x)+\cdots+u^{k-1}l_{k-3}(x)), \ldots, x^{r_2-r_3-1}$ $(u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x)), \ldots, u^{k-1}a_{k-1}(x), xu^{k-1}a_{k-1}(x), \ldots,$ $x^{n-r_k-1}u^{k-1}a_{k-1}(x)\}$. As in the proof of part 2 of Theorem 3.1, it is suffices to show that $u^{k-1}x^{r_{k-1}-r_k}a_{k-1}(x) \in \text{span}(B_2)$. Let the leading coefficients of $x^{r_{k-1}-r_k}a_{k-1}(x)$ be a_0 and of $g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)$ be g_0. There exists a constant $c_0 \in \mathbb{Z}_p$ such that $a_0 = c_0g_0$. Then we have

$$u^{k-1}x^{r_{k-1}-r_k}a_{k-1}(x) = u^{k-1}c_0(g(x) + up_1(x) + \cdots + u^{k-1}p_{k-1}(x)) + u^{k-1}m(x),$$

where $u^{k-1}m(x)$ is a polynomial in C_k of degree less than r_{k-1}. Any polynomial in C_k must have degree greater or equal to deg $(u^{k-1}a_{k-1}(x)) = r_k$. Hence, $r_k \leq$ deg $m(x) < r_{k-1}$ and $u^{k-1}m(x) = \alpha_0u^{k-1}a_{k-1}(x) + \alpha_1xu^{k-1}a_{k-1}(x) + \cdots + \alpha_{r_{k-1}-r_k-1}x^{r_{k-1}-r_k-1}u^{k-1}a_{k-1}(x)$. Thus, $u^{k-1}x^{r_{k-1}-r_k}a_{k-1}(x) \in \text{span}(B_2)$. Hence B_2 is a generating set. As in (1), by comparing the coefficients we can see that B_2 is linearly independent. Therefore, B_2 is a minimal spanning set.
(3) This case is a special case of (2), so the proof is similar to case (2). □

4. Minimum distance

Let n is not relatively prime to p. Let $C_2 =< g(x) + up(x), ua(x) >$ be a cyclic code of length n over $R_2 = \mathbb{Z}_p + u\mathbb{Z}_p, u^2 = 0$. We define $C_{2,u} = \{k(x) \in R_{2,n} : uk(x) \in C_2\}$. It is easy to see that $C_{2,u}$ is a cyclic code over $\mathbb{Z}_p$. Let C_k be a cyclic code of length n over $R_k = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p, u^k = 0$. We define $C_{k,u^{k-1}} = \{k(x) \in R_{k,n} : u^{k-1}k(x) \in C_k\}$. Again it is easy to see that $C_{k,u^{k-1}}$ is a cyclic code over $\mathbb{Z}_p$.

Theorem 4.1. *Let n is not relatively prime to p. If $C_k =< g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x), ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x), u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x), \ldots, u^{k-2}a_{k-2}(x) + u^{k-1}t_1(x), u^{k-1}a_{k-1}(x) >$ is a cyclic code of length n over $R_k = \mathbb{Z}_p + u\mathbb{Z}_p + \cdots + u^{k-1}\mathbb{Z}_p, u^k = 0$. Then $C_{k,u^{k-1}} =< a_{k-1}(x) >$ and $w_H(C_k) = w_H(C_{k,u^{k-1}})$.*

Proof. We have $u^{k-1}a_{k-1}(x) \in C_k$, thus $< a_{k-1}(x) >\subseteq C_{k,u^{k-1}}$. If $b(x) \in C_{k,u^{k-1}}$, then $u^{k-1}b(x) \in C_k$ and hence there exist polynomials $b_1(x), \dots, b_k(x) \in \mathbb{Z}_p[X]$ such that $u^{k-1}b(x) = b_1(x)u^{k-1}g(x) + b_2(x)u^{k-1}a_1(x) + b_2(x)u^{k-1}a_2(x) + \cdots + b_k(x)u^{k-1}a_{k-1}(x)$. Since $a_{k-1}(x)|a_{k-2}(x)| \dots |a_2(x)|a_1(x)|g(x)$, we have $u^{k-1}b(x) = m(x)u^{k-1}a_{k-1}(x)$ for some polynomial $m(x) \in \mathbb{Z}_p[x]$. So, $C_{k,u^{k-1}} \in < a_{k-1}(x) >$, and hence $C_{k,u^{k-1}} =< a_{k-1}(x) >$. Let $m(x) = m_0(x) + um_1(x) + \cdots + u^{k-1}m_{k-1}(x) \in C_k$, where $m_0(x), m_1(x), \dots, m_{k-1}(x) \in \mathbb{Z}_p[x]$. We have $u^{k-1}m(x) = u^{k-1}m_0(x)$, $w_H(u^{k-1}m(x)) \leq w_H(m(x))$ and $u^{k-1}C_k$ is subcode of C_k with $w_H(u^{k-1}C_k) \leq w_H(C_k)$. Therefore, it is sufficient to focus on the subcode $u^{k-1}C_k$ in order to prove the theorem. Since $u^{k-1}C_k =< u^{k-1}a_{k-1}(x) >$, we get $w_H(C_k) = w_H(C_{k,u^{k-1}})$. □

Definition 4.2. *Let $m = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_1p + b_0$, $b_i \in \mathbb{Z}_p, 0 \leq i \leq l-1$, be the p-adic expansion of m.*

(1) *If $b_{l-i} \neq 0$ for all $1 \leq i \leq q, q < l$, and $b_{l-i} = 0$ for all $i, q+1 \leq i \leq l$, then m is said to have a p-adic length q zero expansion.*
(2) *If $b_{l-i} \neq 0$ for all $1 \leq i \leq q, q < l$, $b_{l-q-1} = 0$ and $b_{l-i} \neq 0$ for some $i, q+2 \leq i \leq l$, then m is said to have p-adic length q non-zero expansion.*
(3) *If $b_{l-i} \neq 0$ for $1 \leq i \leq l$, then m is said to have a p-adic length l expansion or p-adic full expansion.*

Lemma 4.3. *Let C be a cyclic code over R_k of length p^l where l is a positive integer. Let $C =< a(x) >$ where $a(x) = (x^{p^{l-1}} - 1)^b h(x)$, $1 \leq b < p$. If $h(x)$ generates a cyclic code of length p^{l-1} and minimum distance d then $d(C) = (b+1)d$.*

Proof. For $c \in C$, we have $c = (x^{p^{l-1}} - 1)^b h(x)m(x)$ for some $m(x) \in \frac{R_k[x]}{(x^{p^l}-1)}$. Since $h(x)$ generates a cyclic code of length p^{l-1}, we have $w(c) = w((x^{p^{l-1}} - 1)^b h(x)m(x)) = w(x^{p^{l-1}b}h(x)m(x)) + w({}^bC_1 x^{p^{l-1}(b-1)}h(x)m(x)) + \cdots + w({}^bC_{b-1} x^{p^{l-1}}h(x)m(x)) + w(h(x)m(x))$. Thus, $d(c) = (b+1)d$. □

Theorem 4.4. *Let C_k be a cyclic code over R_k of length p^l where l is a positive integer. Then, $C_k =< g(x) + up_1(x) + u^2p_2(x) + \cdots + u^{k-1}p_{k-1}(x), ua_1(x) + u^2q_1(x) + \cdots + u^{k-1}q_{k-2}(x), u^2a_2(x) + u^3l_1(x) + \cdots + u^{k-1}l_{k-3}(x), \dots, u^{k-2}a_{k-2}(x) + u^{k-1}t_1(x), u^{k-1}a_{k-1}(x) >$ where $g(x) = (x-1)^{t_1}, a_1(x) = (x-1)^{t_2}, \dots, a_{k-1}(x) = (x-1)^{t_k}$. for some $t_1 > t_2 > \cdots > t_k > 0$.*

(1) *If $t_k \leq p^{l-1}$, then $d(C) = 2$.*
(2) *If $t_k > p^{l-1}$, let $t_k = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_1p + b_0$ be the p-adic expansion of t_k and $a_{k-1}(x) = (x-1)^{t_k} = (x^{p^{l-1}} - 1)^{b_{l-1}}(x^{p^{l-2}} - 1)^{b_{l-2}} \cdots (x^{p^1} - 1)^{b_1}(x^{p^0} - 1)^{b_0}$.*
    (a) *If t_k has a p-adic length q zero expansion or full expansion ($l = q$). Then, $d(C_k) = (b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$.*
    (b) *If t_k has a p-adic length q non-zero expansion. Then, $d(C_k) = 2(b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$*

Proof. The first claim easily follows from Theorem 2.6. From Theorem 4.1, we see that $d(C_k) = d(u^{k-1}C_k) = d((x-1)^{t_k})$. hence, we only need to determine

the minimum weight of $u^{k-1}C_k = (x-1)^{t_k}$.
(1) If $t_k \le p^{l-1}$, then $(x-1)^{t_k}(x-1)^{p^{l-1}-t_k} = (x-1)^{p^{l-1}} = (x^{p^{l-1}}-1) \in C_k$. Thus, $d(C_k) = 2$.
(2) Let $t_k > p^{l-1}$. (a) If t_k has a p-adic length q zero expansion, we have $t_k = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_{l-q}p^{l-q}$, and $a_{k-1}(x) = (x-1)^{t_k} = (x^{p^{l-1}} - 1)^{b_{l-1}}(x^{p^{l-2}}-1)^{b_{l-2}} \cdots (x^{p^{l-q}}-1)^{b_{l-q}}$. Let $h(x) = (x^{p^{l-q}}-1)^{b_{l-q}}$. Then $h(x)$ generates a cyclic code of length p^{l-q+1} and minimum distance $(b_{l-q}+1)$. By Lemma 4.3, the subcode generated by $(x^{p^{l-q+1}}-1)^{b_{l-q+1}}h(x)$ has minimum distance $(b_{l-q+1}+1)(b_{l-q}+1)$. By induction on q, we can see that the code generated by $a_{k-1}(x)$ has minimum distance $(b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$. Thus, $d(C_k) = (b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$.
(b) If t_k has a p-adic length q non-zero expansion, we have $t_k = b_{l-1}p^{l-1} + b_{l-2}p^{l-2} + \cdots + b_1p + b_0, b_{l-q-1} = 0$. Let $r = b_{l-q-2}p^{l-q-2} + b_{l-q-3}p^{l-q-3} + \cdots + b_1p + b_0$ and $h(x) = (x-1)^r = (x^{p^{l-q-2}}-1)^{b_{l-q-2}}(x^{p^{l-q-3}}-1)^{b_{l-q-3}} \cdots (x^{p^1} - 1)^{b_1}(x^{p^0}-1)^{b_0}$. Since $r < p^{l-q-1}$, we have $p^{l-q-1} = r + j$ for some non-zero j. Thus, $(x-1)^{p^{l-q-1}-j}h(x) = (x^{p^{l-q-1}}-1) \in C_k$. Hence, the subcode generated by $h(x)$ has minimum distance 2. By Lemma 4.3, the subcode generated by $(x^{p^{l-q}}-1)^{b_{l-q}}h(x)$ has minimum distance $2(b_{l-q}+1)$. By induction on q, we can see that the code generated by $a_{k-1}(x)$ has minimum distance $2(b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$. Thus, $d(C_k) = 2(b_{l-1}+1)(b_{l-2}+1)\cdots(b_{l-q}+1)$. □

5. Examples

Example 5.1. *Cyclic codes of length* 5 *over* $R_4 = \mathbb{Z}_3 + u\mathbb{Z}_3 + u^2\mathbb{Z}_3 + u^3\mathbb{Z}_3, u^4 = 0$*: We have*

$$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1) = g_1g_2 \text{ over } R_4.$$

The non-zero cyclic codes of length 5 *over* R_4 *with generator polynomial are given in Table 1.*

Table 1. Cyclic codes of length 5 over R_4.

Non-zero generator polynomials
$< 1 >, < g_1 >, < g_2 >$
$< u >, < ug_1 >, < ug_2 >$
$< u^2 >, < u^2g_1 >, < u^2g_2 >$
$< u^3 >, < u^3g_1 >, < u^3g_2 >$
$< g_1, u >, < g_2, u >, < g_1, u^2 >, < g_2, u^2 >, < g_1, u^3 >, < g_2, u^3 >$
$< ug_1, u^2 >, < ug_2, u^2 >$
$< u^2g_1, u^3 >, < u^2g_2, u^3 > .$

References

[1] Taher Abualrub, Ali Ghrayeb, and Robert H. Oehmke. A mass formula and rank of $\mathbb{Z}_4$ cyclic codes of length 2^e. *IEEE Trans. Inform. Theory*, 50(12):3306–3312, 2004.
[2] Taher Abualrub and Robert Oehmke. On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e. *IEEE Trans. Inform. Theory*, 49(9):2126–2133, 2003.

[3] Taher Abualrub and Irfan Siap. Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$. *Des. Codes Cryptogr.*, 42(3):273–287, 2007.

[4] Mohammed Al-Ashker and Mohammed Hamoudeh. Cyclic codes over $Z_2+uZ_2+u^2Z_2+\cdots+u^{k-1}Z_2$. *Turkish J. Math.*, 35(4):737–749, 2011.

[5] Thomas Blackford. Cyclic codes over Z_4 of oddly even length. *Discrete Appl. Math.*, 128(1):27–46, 2003. International Workshop on Coding and Cryptography (WCC 2001) (Paris).

[6] A. Bonnecaze and P. Udaya. Cyclic codes and self-dual codes over $F_2 + uF_2$. *IEEE Trans. Inform. Theory*, 45(4):1250–1255, 1999.

[7] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic cyclic codes. *Des. Codes Cryptogr.*, 6(1):21–35, 1995.

[8] A. Robert Calderbank, Eric M. Rains, P. W. Shor, and Neil J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[9] J. H. Conway and N. J. A. Sloane. Self-dual codes over the integers modulo 4. *J. Combin. Theory Ser. A*, 62(1):30–45, 1993.

[10] Steven T. Dougherty and Keisuke Shiromoto. Maximum distance codes over rings of order 4. *IEEE Trans. Inform. Theory*, 47(1):400–404, 2001.

[11] Vera S. Pless and Zhongqiang Qian. Cyclic codes and quadratic residue codes over Z_4. *IEEE Trans. Inform. Theory*, 42(5):1594–1600, 1996.

[12] J. H. van Lint. Repeated-root cyclic codes. *IEEE Trans. Inform. Theory*, 37(2):343–345, 1991.

Department of Applied Mathematics, Indian School of Mines, Dhanbad 826 004, India

E-mail address: `singh.ak.am@ismdhanbad.ac.in, kewat.pk.am@ismdhanbad.ac.in`